State of Montana Information Security Advisory Council

Council Meeting Minutes
October 27, 2016
11:00 a.m.
Mitchell Room 7

Members Present:
Ron Baldwin CIO/SITSD, Chair
Lynne Pizzini, CISO/SITSD
Joe Frohlich, SITSD
John Burrell, Justice/MATIC Alternate
John Daugherty, DOC
Kreh Germaine, DNRC
Jim Gietzen, OPI
Joe Chapman, DOJ
Craig Stewart, DMA Alternate

Staff Present:
Jennifer Schofield, Wendy Jackson

Guests Present:
Suzi Kruger, Lance Wetzel, Tim Kosena, Dawn Temple, Carroll Benjamin

🖱 **Real-time Communication:**
John Cross, Zach Day, Phillip English, Josh Rutledge, Manual Soto, Terry Meagher, Erin Stroop, Edwina Morrison, Daniel Nelson, Manual Soto, Eric Durkin, Dave Johnson, Josh Rutledge, Jessica Plunkett, Mike Mazanec, Edward Sivils, Christi Mock

Welcome and Introductions

Ron Baldwin welcomed the council to the October 27, 2016 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes

Lynne Pizzini made a motion to approve September 15, 2016 minutes as presented. John Daugherty seconded the motion. Motion carried.

Business

MT-ISAC Schedule – Day / Time Change

Joe Frohlich introduced options for rescheduling the time and day of the MT-ISAC meetings. MT-ISAC will continue to meet throughout the legislative session.

Joe Chapman made a motion that the MT-ISAC meeting be held on the second Wednesday of each month from 1:00 PM to 3:00 PM effective January 2017. Jim Gietzen seconded the motion. Motion passed.

Upcoming Legislative Session

Mr. Baldwin stated that there will be no House Bill 10. There is a House Joint Resolution 21 that is oriented towards privacy. Mr. Frohlich, Ms. Pizzini, and Mr. Baldwin will provide the council with more information concerning House Joint Resolution 21 as it becomes available. MT-ISAC will monitor and provide feedback for legislation that is proposed or carried during the next legislative session. Mr. Baldwin requested that MT-ISAC members bring any pending legislation pertaining to security to the attention of the council.

Mr. Frohlich stated that the pending Department of Revenue (DOR) fraud prevention legislation will not be forwarded for legislative action.

October Cyber Security Awareness Month Activities

Mr. Frohlich gave an update on National Cyber Security Awareness Month, which is a collaborative campaign sponsored by the Department of Homeland Security (DHS) and the National Cyber Security Alliance. Governor Bullock has signed a letter of support for Cyber Security Awareness Month. SANS Securing the Human training has been reset this month for all state employees. All county employees will start the SANS training as well. The theme for the Enterprise Security Program is "It's a Jungle Out There, Be Cyber Security

Aware". The Enterprise Security Program can conduct Cyber Security Events at agency locations upon request. Mr. Frohlich discussed and demonstrated the Cyber Security games, activities and prizes that are available.

Q: Joe Chapman: Has there been any thought towards providing the option to test out of Cyber Security training? The length of this training can be cumbersome and may result in a lack of attention to the subject matter.

A: Mr. Frohlich: The length of the annual training has been shortened to under one hour. Agencies can add on additional training if they wish. This training is updated and revised each year but there are certain topics that need to be addressed annually. Other training platforms would be considered but cost and tracking capability would be essential.

John Daugherty commented that there have been issues of employees starting the training video, walking away, and returning for the question portion of the training. Although there are some updates to this training every year, it is repetitive and can become boring to some individuals.

Stuart Fuller stated that he has encountered this issue as well. Allowing for a larger window of time for this training to be completed may be helpful.

Ms. Pizzini stated that the requirement states that individuals take the training annually. Testing out of certain areas might not meet this training requirement. This training is required for insurance purposes.

Action Item: Mr. Baldwin stated that SITSD will look into revising this training to make it less repetitive and more engaging.

Workgroup Updates

Best Practices / Tools Workgroup

Ms. Pizzini stated that the Vulnerability Management Best Practice was posted in September. There have been no written comments submitted.
Mr. Daugherty commented that, under the removal of affected software on page 4, section 3, verbiage should be added to specify that software should be removed when it deprecates.

Ms. Pizzini moved that the council accept this document, with Mr. Daugherty's addition, as a Best Practice. Mr. Daugherty seconded the motion. Motion passed.

Ms. Pizzini stated that the workgroup has make changes to Acceptable Use Best Practice document to add verbiage directing that this document be used for the onboarding of all employees. This document also identifies the rules of behavior for state employees and contractors. This document is posted for review by the council and will be voted on at the next MT-ISAC meeting.

Mr. Frohlich gave an update on the Data Loss Prevention Workgroup. At this time, Data Loss Prevention is focusing on One Drive for Business and SharePoint online. Exchange is still in the testing phase. A single template will be applied to all agencies that will identify social security or credit card information included in a document and alert the user. This template will inhibit the sharing of sensitive information outside of the state network. It is still being determined how this information might be shared within state agencies as there is some need for sharing of sensitive information within the state agency network. Mr. Frohlich requested that agencies submit a ticket to the service desk requesting Data Loss Prevention testing so they can see how this template relates to their business needs. November 21, 2016 is the date for Data Loss Prevention to go live for SharePoint online and One Drive for Business.
Ms. Pizzini commented that MT-ISAC will be making a recommendation as to how those templates are set up. It is important that each agency participate in the testing so that their MT-ISAC representatives can provide input on how the templates should be set up.

Ms. Pizzini gave an update on the Special Workgroup for Enterprise Endpoint Protection. This workgroup has reviewed the information gathered in the Request for Information (RFI) and is recommending the pursuit of an Enterprise Solution for an add-on to anti-virus to help protect desktops. The workgroup will put together the business requirements and develop an Enterprise recommendation where the agencies can purchase and

implement an add-on to anti-virus.
Mr. Frohlich added that the workgroup has decided to stay with Microsoft for Endpoint Protection. September 2017 will be the last month for those agencies that have ESET to move towards the Microsoft Endpoint Protection for desktops as it is part of the Enterprise Agreement with Microsoft, which is part of the enterprise rate. Microsoft Endpoint Protection will be the Enterprise AV for desktops starting in September 2017. Sophos will be the Enterprise AV for Servers starting in September 2017. Those agencies who have ESET for Linux servers are encouraged to move to Sophos as soon as SITSD has appropriate licensing. The agreement with ESET has been renewed for one year to allow agencies time to transition to Sophos for servers and Microsoft Endpoint Protection for desktops. Agencies should start their planed migration to Microsoft Endpoint now for desktops. For servers that agencies host themselves that are not apart the shared SITSD environment (agency that has physical server or VSP) it is the agencies responsibility to migrate to Sophos by September 2017. If the server is hosted by SITSD and managed by SITSD then the server will be migrated to Sophos by SITSD. Linux servers will have priority for licensing prior to July 1 2017. Starting fiscal year 2018 (July 1, 2017), there will be licensing for all servers to move to Sophos. Sophos Server licenses are purchased by SITSD, there will be no charge to the agencies for server AV. The ESET cost for desktops will be passed to agencies. Microsoft Endpoint Protection for desktop AV is a part of the EA and there will be no additional costs to agencies for the desktop AV.

Situational Awareness Workgroup
John Burrell commented that the Situational Awareness Workgroup met on October 26, 2016 to discuss the process of sharing information with private sector, critical infrastructure entities. The workgroup will discuss what that process will include and what information can be shared, insuring that sensitive information is not passed into the private sector. This workgroup will consult with MT-ISAC to identify a template that can be used to develop sharing agreements.

Open Forum
Joe Frohlich reviewed the process for disposal of storage media and destruction of hard drives. This process requires that the storage media be destroyed onsite. The only hard drive shredder in Helena is at the vendor's site. Fish Wildlife and Parks (FWP) has raised the question of how this is going to be addressed as an enterprise solution.
Mr. Fuller observed that the state is at risk of incurring to fines due to violation of HIPPA if they fail to establish a Business Associate Agreement with the vendor who destroys these devices.
Ms. Pizzini stated that an SITSD should pursue an Enterprise Agreement to ensure full compliance with the law.

Action Item: Ms. Pizzini and Mr. Frohlich will pursue an Enterprise Agreement with the vendor responsible for hard drive destruction to ensure full compliance with the law regarding disposal of storage media.

Stuart Fuller stated that many government and private sector entities are utilizing Google Docs, which are blocked by the filter. As a result, there are several requests for exceptions to this block. Mr. Fuller inquired as to how many blocks and exceptions are in place and what risks are associated with Google Docs?

Action Item: Ms. Pizzini stated that research will be done to investigate current security concerns for Google Docs and the number of exceptions that exist and bring that information back to MT-ISAC for discussion.

Future Agenda Items
Cyber Security Insurance; procedures and training/reporting requirements

Public comment
None

<u>Adjournment</u> Next Meeting
Thursday November 17, 2016
11:00 AM to 1:00 PM
Mitchell Room 7

Adjourn

The meeting was adjourned at 12:23 PM